Tanıtım – Değerlendirme / *Reviews*

Henkoğlu, T. (2015). *Bilgi güvenliği ve kişisel verilerin korunması.* Yetkin Yayınları, Ankara. ISBN: 978-975-464-982-6.

Dilan Şerife Şişkin*

Book Review

Information security and protection of personal data

Türkay Henkoğlu, who studies on sensitive and personal data, published a book entitled "Information security and protection of personal data" in 2015. In this book, subjects related to information security personal data protection were evaluated within the context of a comprehensive information security model and legal conditions. Furthermore, 15 information centers in universities located in Ankara were analyzed in terms of their current approaches regarding information security policy and legal regulations.

Hassas ve kişisel veriler üzerine çalışmaları bulunan Dr. Türkay Henkoğlu tarafından yazılan "Bilgi güvenliği ve kişisel verilerin korunması" başlıklı kitap, Yetkin Yayınevi tarafından 2015 yılında yayımlanmıştır. Kitap içeriği incelendiğinde bilgi güvenliği ve kişisel verilerin korunmasına ilişkin hususların hem kapsamlı bir bilgi güvenliği modeli hem de hukuksal koşullar çerçevesinde değerlendirildiği görülmektedir. Bununla birlikte, Ankara'da bulunan 15 üniversitenin bilgi merkezlerindeki mevcut uygulamalar hassas ve kişisel verilerin korunması, yasal ve hukuksal düzenlemeler çerçevesinde analiz edilmiştir. Araştırma verilerinden hareketle araştırmanın sonunda üniversiteler için bir bilgi politikası geliştirilmiştir. Eserde yer alan bilgi politikasının Türkiye'deki üniversiteler için yol gösterici bir rehber olduğunu söylemek mümkündür. Nitekim ikinci bölümünde sunulan araştırma bulguları da bu eksikliği açıkça ortaya koymaktadır. Bunun yanı sıra kitabın bilgi merkezlerinde kişisel verilerin korunması konusunda sınırlı sayıda çalışmanın bulunduğu literatüre önemli bir katkı sağladığı aşikârdır. Ayrıca günümüzde dijitalleşme, bilginin mahremiyeti ve kişisel verilerin

* Yüksek lisans öğrencisi. Hacettepe Üniversitesi, Bilgi ve Belge Yönetimi Bölümü, e-posta: dilansiskin@hacettepe.edu.tr
Graduate student. Hacettepe University, Department of Information Management, Turkey.

Geliş Tarihi - *Received*: 31.08.2018
Kabul Tarihi - *Accepted*: 16.10.2018

korunması gibi konulardaki teknik ve yasal düzenlemelerin kütüphanecilik ve bilgi bilim alanına farklı bir yön vermeye başladığını söylemek mümkündür.

Kitabın başında önsöz, içindekiler ve kısaltmalar yer alırken sonunda ise bilgi güvenliğine yönelik zengin bir kaynakça yer almaktadır. Burada önsöz incelendiğinde (s.9), Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümü Anabilim Dalında Prof. Dr. Nazan Özenç Uçak danışmanlığında 2015 yılında tamamlanmış olan "Hassas bilgi varlıklarının ve kişisel verilerin hukuksal düzenlemeler ile korunması ve bu kapsamda üniversiteler için bilgi güvenliği politikasının geliştirilmesi" başlıklı doktora tezine[1] dayandığı anlaşılmaktadır. Diğer taraftan, yazarın üslubunun anlaşılır ve yalın olduğu görülmektedir. Bilimsel kaynakça yazım kurallarından American Psychological Association (APA) 5. baskıya göre yazılan kitabın bibliyografyası, ele alınan konunun ulusal ve uluslararası boyutta hukuki ve yasal olarak işlendiğini bir kez daha ortaya koymaktadır. Buna ek olarak, eserin biçimsel ve anlamsal açıdan düzenine oldukça önem verilmiştir. Bölümlerde verilen dipnotlar ise ele alınan konuların daha rahat anlaşılmasını sağlamanın yanı sıra ilgili konuların detaylarını görmek isteyen okuyucular için de bir yol gösterici nitelik taşımaktadır.

Bilgi ve belge yönetimi alanına farklı bir perspektif getiren bu eserin temaları, üç ana bölümde okuyucuya sunulmuştur. Kitabın birinci ana bölümünde hassas bilgi varlıklarının ve kişisel verilerin korunması konusu yedi alt başlıkta anlatılmaktadır. Birinci alt başlıkta, üniversitelerde hassas ve kişisel verilerin, alınan bilgi güvenliği önlemlerinin ve bilgi güvenliği politikalarının yetersizliği ve literatürdeki diğer çalışmalarda değinilmeyen konular vurgulanarak kitabın taşımış olduğu özgün değer açıklanmıştır. Bölümün ikinci alt başlığında kişisel verilerin korunmasının önemine değinilmiştir. *"1.2. Kişisel Verilerin Korunması"* başlığını taşıyan bu alt bölümde (s. 26) literatürde yapılmış çalışmalardaki eksiklikler şu şekilde ifade edilmiştir:

> *"Kişisel verilerin korunması konusunda hukuk alanı dışında yapılan ve daha geniş boyutta alınabilecek çalışmalar yok denecek kadar azdır. Kurum ve kuruluşların kişisel verilerin korunmasını da amaçlayan kapsamlı bilgi güvenliği politikalarından yoksun olmalarının en önemli nedenlerinden biri, bu konuda örnek alınabilecek çalışmaların bulunmamasıdır. Bir kurum ya da kuruluş için kapsamlı bilgi güvenliği politikası geliştirebilmesi için, bu konudaki tüm koşulların değerlendirildiği araştırma sonuçlarına gereksinim duyulmaktadır. Özellikle yeni açılan üniversitelerde bilgi yönetim süreçleri ve bilgi güvenliği sorumluluklarına ilişkin eksikliklerin tespit edilerek bu konuda rehber ilkelerin oluşturulması, diğer kurum ve kuruluşlara istihdam sağlayan öncü ve örnek kuruluşlar olarak üniversitelerde standartların belirlenmesi açısından önem taşımaktadır."*

Kitapta ele alınan konunun önemine vurgu yapan bu bölümün ardından yine konuyla ilgili temel kavramların açıklandığı üçüncü alt başlık verilmiştir. Bu başlıkta veri, bilgi ve kişisel veri ilişkisi üzerinde durulmuştur. Dördüncü alt başlıkta, McCumber tarafından 1991 yılında geliştirilen ve bilgi güvenliğini kavramsal açıdan ayrıntılı bir şekilde sunan bilgi güvenliği modeli ele alınmıştır. Beşinci alt başlıkta, kişisel verilerin korunmasına ilişkin hukuksal düzenlemeler Avrupa Birliği mevzuatı çerçevesinde değerlendirilmiştir. Türk hukuk mevzuatında kişisel ve hassas verilerin korunmasına yönelik düzenlemeler ise bu bölümün bir

[1] bkz. http://www.bby.hacettepe.edu.tr/yayinlar/dosyalar/henkoğlu.pdf

diğer alt başlığını oluşturmuştur. Son alt başlıkta, kişisel ve hassas verilerin korunmasına ilişkin hukuksal düzenlemeler McCumber bilgi güvenliği modeli çerçevesinde değerlendirilmiştir.

İkinci ana bölümde, Ankara'da yer alan 15 üniversitenin Bilgi İşlem Daire Başkanlığı (BİDB), Personel Daire Başkanlığı (PDB) ve bilgi merkezindeki bilgi güvenliği ve risk yönetimine yönelik uygulamalar betimlenmiştir. Araştırmadaki veriler ilgili üç birimin daire başkanları ya da yardımcılarından toplanmıştır. Diğer taraftan, araştırmanın denekleri sadece gerçek kişi ile ilişkili olup, veri sahibi olarak isimlendirilen kurum ve kuruluşlar araştırmanın kapsamına dâhil edilmemiştir. Betimleme yöntemine dayanan araştırmada görüşme ve anket teknikleri kullanılmıştır. Çalışmada öncelikli olarak, üniversitelerin web sitelerindeki içerikler kişisel verilerin korunmasıyla bağlantılı olarak analiz edilmiştir. Bu ön incelemede (s.120), üniversitelerde veri akışının en yoğun olarak işlendiği birimlerin PDB ve bilgi merkezi olarak adlandırılan üniversite kütüphaneleri olduğu vurgulanmıştır. Bu analizlerde elde edilen bir diğer sonuç ise, bilgi güvenliğini sağlamaya ilişkin sorumluluğun tüm üniversitelerde BİDB'e verildiği ve bu nedenle bilgi güvenliği önlemlerinin alınmasına yönelik çalışmaların sadece üniversitelerin BİDB tarafından yürütüldüğüdür. Dahası, bilgi güvenliği gibi önemli bir konunun sadece BİDB'e verilmesinin yanı sıra üniversitelerde personel ve öğrencilere ait kişisel verileri işleyen üniversite PDB ve bilgi merkezlerinin web sayfalarında, bu verilerin işlenmesine ve korunmasına yönelik politika ve etik ilkelerin bulunmadığı tespit edilmiştir. Diğer taraftan, üniversite etik kurul yönergelerinde de bu konuya ilişkin ifadelere yer verilmemesi ve gereken etik duyarlılığın gösterilmemesi bilgi güvenliği gibi hassas bir konunun üniversiteler tarafından önemsenmediğini ortaya çıkartmıştır. Bu araştırmada kullanılan diğer bir yöntem ise, doküman analizi yöntemi olmuştur. Araştırma kapsamında uygulanan bu yöntemde ise, hassas ve kişisel verilerin korunmasına ilişkin mevcut durumu ortaya koymak amacıyla öncelikle literatürdeki çalışmalar değerlendirilmiş ve hassas bilgi varlıklarının ve ve kişisel verilerin korunmasına ilişkin şartları içeren AB Hukuk Mevzuatı ve Türk Hukuk Mevzuatı incelenmiştir. Bununla birlikte, üniversitelerin içinde bulundukları riskler de bu araştırmada ele alınmıştır.

Kitap içeriğinde sunulan araştırma, üniversitelerde kişisel verilerin korunmasına yönelik yasal düzenlemelerin, bilgi güvenliği politikalarının ve kişisel verilerin işlenmesi ve korunması ile ilgili personele eğitim ve farkındalık çalışması yapılmadığını ortaya koymuştur. Bu bölümde ayrıca, kişisel verilerin toplanması, düzenlenmesi ve saklanması, kişisel verilerin kullanımı ve paylaşımı, kişisel verilerin korunmasına ilişkin bilgi güvenliği önlemleri, kişisel verilerin korunmasına ilişkin önlemlerin standartlar ve yasalara uyumluluğu, kişisel verilerin depolanması ve korunmasına ilişkin sorumluluklar, üniversite kurum ve kuruluşlarda risk yönetimi, kişisel verilerin imha edilmesi ve sistem kayıtlarının temizlenmesi, bilgi güvenliğinin sağlanması ile ilgili eğitim uygulamaları, konuyla ilgili farkındalık ve kişisel verilerin korunmasına ilişkin görüş ve önerilere yer verilmiştir.

Araştırmanın son bölümü olan üçüncü bölümde, üniversiteler için geliştirilen bilgi politikasına yer verilmiştir. Politika içeriğinde öncelikle bir yönergede de bulunabilecek başlıkların sunulduğu görülmektedir. Bu kapsamda politikada ilk olarak amaç, kapsam, kısaltma ve tanımlar, yetki ve sorumluluklar gibi başlıklara yer verilmiştir. Bunun ardından ise politikada üniversitelerde bilgi güvenliği risk yönetim stratejisinin geliştirilmesi, bilgi güvenliği önlemleri, hukuksal düzenlemeler ve temel ilkeler kapsamında kişisel verilerin ve bireyin korunması, eğitim programları, veri ihlali yönetim planı ve denetimlere ilişkin hususlar,

yaptırımlar ve ilgili politikalar ve yol haritası başlıkları sıralanmıştır. Yirmi üç sayfa ve on alt başlıktan oluşan bilgi güvenliği politikasının sonunda ise kitapta yer alan bilgi güvenliği önlemlerinin üniversitelerin kendi özel koşullarını değerlendirerek geliştirecekleri bilgi güvenliği için öneri ve kaynak niteliğinde olduğuna vurgu yapılmıştır.

Üniversitelerde, kişisel verilerin ve bilgi varlıklarının sürekli olarak üretildiği ya da sağlandığı, bu verilerin iş süreçleri, bilimsel araştırma ya da eğitim gibi amaçlarla işlendiği ve bu verilerin saklandığı birimlerden biri bilgi merkezleridir. Bu merkezlerdeki verilerin korunması ve güvenliğinin sağlanması birden çok birimin ve bölümün işbirliği içerisinde çalışmasını gerektirmektedir. Diğer taraftan bilginin kolaylıkla paylaşılması ve değiştirilebilmesi, dijitalleştirmenin getirdiği güvenlik açıkları, kişisel verilerin daha yoğun olarak dijital ortamda tutulması, siber-saldırılar gibi nedenler bilgi merkezlerinde bilgi güvenliğinin ve risk analizlerinin yapılması, mevcut insan kaynaklarının (karar verici, profesyoneller ve kullanıcılar) konuyla ilgili eğitilmesi ve farkındalıklarının yaratılmasını zorunlu hale getirmiştir. Dolayısıyla, üniversite kütüphanelerinde oluşabilecek risklerin önlenmesi ya da gerekli bilgi güvenliği uygulamalarının sürdürülebilir bir yapıda gerçekleştirilmesi açısından sunduğu politika örneğiyle bu kaynak, bilgi güvenliği politikası geliştirme aşamasında bilgi merkezleri için başvurulması gereken bir rehber niteliği taşımaktadır.

Teşekkür

Metni okuyarak öneri ve düzeltmelerde bulunan hocam Dr. Öğretim Üyesi Tolga Çakmak'a ve araştırma kapsamında beni yönlendiren Araştırma Görevlisi Müge Akbulut'a çok teşekkür ederim.